sciendo

Proceedings on Privacy Enhancing Technologies ; 2022 (1):105–125

Maryam Mehrnezhad*, Kovila Coopamootoo*, and Ehsan Toreini

How Can and Would People Protect From Online Tracking?

Abstract: Online tracking is complex and users find it challenging to protect themselves from it. While the academic community has extensively studied systems and users for tracking practices, the link between the data protection regulations, websites' practices of presenting privacy-enhancing technologies (PETs), and how users learn about PETs and practice them is not clear. This paper takes a multidimensional approach to find such a link. We conduct a study to evaluate the 100 top EU websites, where we find that information about PETs is provided far beyond the cookie notice. We also find that opting-out from privacy settings is not as easy as opting-in and becomes even more difficult (if not impossible) when the user decides to opt-out of previously accepted privacy settings. In addition, we conduct an online survey with 614 participants across three countries (UK, France, Germany) to gain a broad understanding of users' tracking protection practices. We find that users mostly learn about PETs for tracking protection via their own research or with the help of family and friends. We find a disparity between what websites offer as tracking protection and the ways individuals report to do so. Observing such a disparity sheds light on why current policies and practices are ineffective in supporting the use of PETs by users.

Keywords: privacy, privacy-enhancing technology, tracking, user-centric, GDPR, tracking protection

DOI 10.2478/popets-2022-0006
Received 2021-05-31; revised 2021-09-15; accepted 2021-09-16.

***Corresponding Author: Maryam Mehrnezhad:** Newcastle University, UK, E-mail: maryam.mehrnezhad@newcastle.ac.uk
***Corresponding Author: Kovila Coopamootoo:** Newcastle University, UK, E-mail: kovila.coopamootoo@newcastle.ac.uk
Ehsan Toreini: Durham University, UK, E-mail: ehsan.toreini@durham.ac.uk

1 Introduction

Today's data-intensive web is characterized by the mining and selling of individuals' data, that enables the provisioning of customised services but unfortunately also engenders targeted advertising [9], digital discrimination [18], privacy-invasive algorithmic computations [24], and a general fuzziness about privacy rights online. In recent years, internet advertising has become increasingly tailored to individual users, and is often referred to as online behavioural advertising or targeted advertising [19]. Online behavioural advertising occurs when advertising networks profile users based on their online activities, and use this profile to show ads that are more likely to be of interest to a particular user [3]. When users visit a web page, the page's content can come from a first- or third-party, where the first-party is the one the user is explicitly visiting, while the third-party includes advertising networks, analytics companies and social networks that contract with first-party websites [47]. While the tracking of user activities can be accomplished in a variety of ways, in the simplest form, the advertiser sets a cookie with a unique identifier on the user's computer [42].

Since the enforcement of the GDPR, most EU websites display cookie consent notices, which are expected to inform users of its cookie use and tracking practices. However, there is scepticism about the effectiveness of cookie notice (aka cookie consent/ banner) for tracking protection. For example, recent investigations found that (1) cookie banners on web pages do not necessarily respect people's choice, in particular, the Do Not Track option on some browsers only serve to declare non-consent and are not respected by web pages [46]; (2) approximately half of the websites, in a large-scale study in Europe, violate the EU cookie directive, by installing profiling cookies before users consent [75]; and (3) dark patterns and implied consent are prevalent in consent management platforms, such that only 11.8% of the top 10k websites in the UK meet the minimal GDPR requirements [53]. There is also an overall lack of usable mechanisms for users to consent or deny the processing of personal data [16].

Users can protect themselves from tracking via a few ways including rejecting the cookie notice, using builtin browser options, browser blocking extensions or other tracking protection privacy-enhancing technologies (PETs). PETs are defined as technologies shaped according to privacy principles, and covers a broad range of technologies that are designed for supporting privacy and data protection [20]. Additionally, a few browsers are designed with the specific aim of blocking tracking activities e.g. Brave browser (brave.com), Tor Browser (torproject.org), and Duckduckgo Browser (duckduckgo.com). In these browsers, the blocking module is a part of the browser engine and tracking is prevented at the time of parsing the web page (or even before that when the browser has received contents with tracking behaviour). The effectiveness of some of these PETs has been studied in the previous work e.g. in [25, 27, 51, 74].

The general public opinion in national surveys as reported in the UK and Europe is that tracking online is a privacy concern for most citizens [5, 10]. However, with regards to the use of PETs for tracking protection, tools and mechanisms have been thought to suffer from usability issues [16, 44, 66]. For general privacy protection, interaction aspects such as knowing that PETs can support privacy [11, 62, 68] and perceiving them as useful [4, 11, 33], are thought to impact usage of PETs, among other factors. In addition, it has been demonstrated that the existing implementation of PETs and in particular cookie notices do not offer fair practices. Many dark patterns have been recognised in the cookie notice of websites, such as with regards to location [77] and user control options [46, 50, 53, 77]. Moreover, limited research is available around other privacy-enhancing information options (beyond cookie notice), where to our knowledge, existing ones mainly address US consumers [12, 31, 32].

Contributions: Evidently, while previous studies have investigated systems and users for tracking practices, the link between the data protection regulations, website practices of presenting PETs in the real-world, and how users learn about PETs and practice them is not clear. Therefore, this paper aims to investigate the links between these three aspects (regulations, systems, and users), as shown in Fig. 1 and by answering these questions: *What are the tracking protection requirements specified in the law? How do websites inform users about PETs for tracking protection and how practical those ways are? How do Internet users learn about PETs for tracking protection and what PETs do they use?*

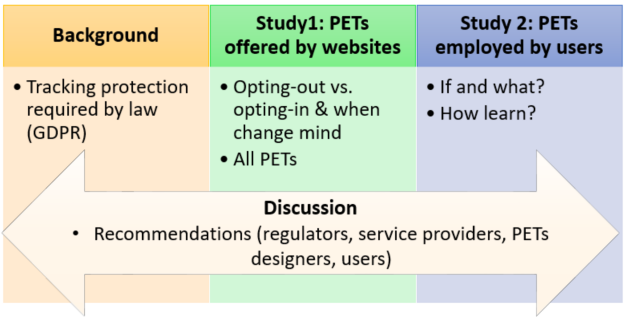

Fig. 1. Overall scope of the paper

We conduct two user-centric studies across three countries in Europe with the highest number of Internet users; the UK, Germany and France. We look at the three aspects of the law, systems, and users and find the disparities (Fig. 1). In Study 1, we investigate whether and how the 100 most used European websites offer tracking protection to users or guide them towards PETs, as required by the GDPR. Study 1 involves a systematic analysis of cookie notices, user options beyond the cookie notice, and an evaluation of the complications for opting-out. This study contributes to the body of knowledge in two ways: (a) it studies the complications of opting-out of previously accepted cookies and (b) it exhaustively reviews the privacy-related content of 100 top EU websites to find all the PETs and their popularity. These two contributions have not been studied in the past. In addition, there is some overlap between this study and the ones conducted in the past. For example, we analyse the cookie notice, control options, and the implications of opting-out [31, 50, 77]. Our findings highlight that: (a) opting-out via cookie consent is much more complicated as opposed to opting-in. More importantly, we find that opting-out from previously accepted privacy settings is much harder than the former and (b) the majority of websites do not offer a fair cookie notice and rely on browser settings by users to prevent tracking. These findings are non-compliant practices, which to the best of our knowledge are studied for the first time.

In Study 2, we seek to gain a broad understanding of the methods Internet users employ for tracking protection online, and how they learn about PETs for tracking protection. We do so via a survey of Internet users themselves, across the three countries (UK, Germany, France) with 614 participants. This study reports on awareness and tracking protection methods employed by users, noting cross-national and gender differences as well as discuss their effectiveness. While most websites

present users with cookie notices, we find that users mostly learn about PETs for tracking protection via their own research or family/friends relations. We also find that UK participants are 34% more likely to not be aware of (or not remember where they could have heard of) PETs for tracking than German and French participants, and women are also 2.7 times more likely to not be aware than men. In addition, we find that women are 74% less likely to find PETs via their own research than men, and German and French participants are twice more likely than UK participants. We report on the use of PETs, categorised as technology type for tracking, noting the preference for browser extensions, manually opting-out and other categories that include ones ineffective for tracking protection.

By providing two user-centric studies from different angles (system evaluation versus user study) and with distinct methodology, we contribute to a comprehensive understanding of user tracking protection in the wild.

2 Background and Related Work

In this section, first, we explain online tracking and protection approaches. Next, we explain what are the regulations for tracking, user rights, and the requirements for websites to meet. And finally, we introduce the related work on the human aspects of tracking protection.

2.1 Online Tracking

Online services companies have gradually designed various ways to collect user data for personalized commercialization. Any device connected to a network can potentially leak information about its users and environment. The rise of connected smart devices (such as smartphones, tablets, and Internet of Things (IoT) devices) has upgraded the online tracking methods to a new level. The most common tracking method is known as *cookies*. Cookies are small pieces of data (in text format) that are downloaded to your device when you visit a website. Other than tracking, cookies are set for different purposes such as remembering user information, authentication across devices, analysing website/application usage, advertising, personalise websites, improving performance and user experience.

Cookies are sent to the client's computer through browsers. The browser is responsible to protect cookies from various threats such as session hijacking, identity theft and more [15]. Therefore, browsers set different permission mechanisms to restrict access to cookies to only eligible parties. The most fundamental cookies protection policy is the principle browser content protection mechanism known as "Same Origin Policy (SOP)" [84]. This policy restricts access to cookie content to merely the domain that generated them. Web server writes the domain section in the HTTP response header before sending the cookie to the client's browser [1]. For online tracking, cookies are divided into two groups: First–party and third–party cookies. First-party cookies are set by the website user is visiting, and only that website can read them (due to the restrictions set by SOP mechanism). In contrast, third-party cookies are set by someone other than the owner of the website. Some web pages may also contain content from other websites (e.g. Google analytic and Twitter) which may set their own cookies. In addition, if you share a link to a page (e.g. Facebook), such a page may set a cookie on your browser. The visited website has no control over third-party cookies; however, due to SOP mechanism, the owner of the third–party cookie has the capability to read the cookie and collect information from the user. The user can turn them off in other ways.

In addition to cookies, a website can *fingerprint* the user's browser [57] based on the information collected through JavaScript (i.e. name of the browser, version, installed extensions, etc.) and the execution platform that the client is browsing with (i.e. smartphone make and model, laptop, screen resolution, etc.). Usually, the fingerprinting information combined with the cookies can provide a well–targeted data collection and tracking of a user. Previous studies demonstrate that many top websites have implemented browser fingerprinting methods to some extend [28]. It is also shown that the browsers are still unreliable to leak tracking information even when the user is browsing through "private mode" [65] through side-channel attacks. Other tracking technologies include web beacons, clear GIFs, page tags and web bugs. They usually take the form of a small, transparent image that is embedded in a webpage or email. They work with cookies and capture data like IP addresses, when the user viewed the page or email, used device, and some form of location data.

In general, users have some degree of control to prevent online tracking. In the browser, users can turn on to request "Do Not Track (DNT)" in the HTTP request. If the server supports this feature, then it will not send cookies to your browser. In practice, this feature is not widely implemented [67]. Also, browser vendors stopped supporting this feature in their products [40].

Users also can install third–party browser extensions to detect tracking behaviour when the page is loading in the browsers. These extensions (e.g. Ghostly and AdBlocker) effectively block a majority of the tracking cookies. Another way to prevent online tracking is to install web browsers with the embedded capability to prevent tracking (e.g. Brave Browser, Tor browser and more). These browsers are more efficient in blocking the tracking behaviour since they are implemented as a part the browser–engine (in contrast to the track–blocking browser extensions which are installed as a third–party extension on top of the browser with more restrictions).

2.2 Regulations

The GDPR [79] came into force in 2018, replacing the old Data Protection Act 1998. It concerns organisations located in the EU as well as those dealing with EU citizens' data around the world. Other data protection regulations include California Consumer Privacy Act (CCPA) [14], the Chinese Personal Information Security Specification (PISS) [56], the Indian Personal Data Protection Bill (PDP Bill) [30], and the Russian Federal Law on Personal Data [49]. We focus on the GDPR since our studies are based on EU websites and users.

The GDPR defines personal data as: "information that relates to an identified or identifiable individual" [37]. To satisfy the GDPR's data protection principles, rights and obligations, it requires the online service providers to tell people that the cookies (or any other similar tracking technologies) are there, explain what the cookies are doing and why, and get the person's consent to use a cookie. The Information Commissioner Officer (ICO) [37] provides extensive guidelines on law-compliant practices. Among other recommendations, ICO's guidelines recommend the service providers to provide a cookie consent which is separated from other matters and does not highlight *Agree* over *Reject* and other options, enable the user to withdraw her/his previously given consent, and do not rely on the browser settings (or other control mechanisms) as their opt-out mechanism. Therefore, providing the user with a fair, independent, and easy mechanism to prevent tracking or change preferences at any time is required by the law.

2.3 Human Aspects

Among the protection strategies for behavioural advertising and tracking online, as categorised via the protection principle they rely on [21], transparency and blocking are the most researched strategies in user studies. Transparency refers to enhancing users' awareness of the tracking of their activities and data, such as via *MyAdChoices*, often accessible via the privacy policy or the cookie consent notice. Blocking refers to limiting undesired interactions with third-parties and inhibiting known tracking mechanisms, and therefore advertising, such as via blockers as *Adblock Plus* or *Ghostery*.

Notice and Choice: Cookie notices of different sets of websites have been studied before [16, 46, 53, 63, 77], and it has been shown that their design (e.g. position, choices) substantially impacts user engagement with them [53, 77]. Similarly, popular designs of cookie notices do not empower the users in terms of control options. Reportedly, and on different detests (PC, mobile, etc.), only around 10% of the websites meet the minimal requirements set by the GDPR [50, 53].

Browser Extensions: Browser extensions vary in effectiveness and can be distinguished between (1) ad blocking extensions that limit ads from being loaded such, as *Adblock Plus*, and (2) tracker blocking extensions that focus on blocking trackers, such as *Ghostery*, *Privacy Badger* or *Disconnect* [51]. In the default settings, these extensions may not effectively block ads and trackers [58] and may need manual configuration for effective protection [80]. Although some extensions have improved their usability, their description in the past was found to be filled with jargon and were not easy for users to change their settings when the tool interfered with websites [43].

Other Tools: Limited research has been conducted to investigate the perception and use of other tracking protection tools. In a recent study [72], the use and perceptions about five web browsing-related tools including private browsing, VPNs, Tor Browser, ad blockers, and antivirus software, have been measured for US users. The results of such research show that the misconceptions may lead the user to use privacy tools for the wrong purpose putting them at potential risks.

2.4 Research Gaps

In addition to human dimensions, some of these studies cover a wide range of other topics including tracking activities [16, 39, 46, 63, 76], tracking on mobile and other smart devices [13, 34, 52, 59, 60, 78], legal aspects [46, 64], and cross-platform evaluations [50, 59, 82]. Various forms of analysis have been performed via different case-studies [31, 53, 77], mainly concerning the consent

notice as the main route of the opt-out and for particular forms of PETs (e.g. data deletion). In contrast, the complication of opting-out of previously accepted privacy settings has not been studied. In addition, little research has gone into all forms of PETs provided by websites in the real-world. Knowing whether or not opting-out from previously accepted privacy settings is as easy as opting-in is particularly important since (1) it is a legal requirement, and (2) certain user groups may become more privacy-aware over time and should be able to modify their privacy settings. In addition, knowing what is the statistics on all forms of PETs offered by websites in the real-world would help to close some of the gaps between real practices of the vendors and end-users. In this paper, we address both via our system studies in Study 1.

Furthermore, knowing that if and what tracking protection is employed by the users contributes to the understanding of the real practices. Previous research has qualitatively elicited protective actions and the use of privacy technologies in general [57, 68], or queried use of specific technologies such as browser extensions [45] and a limited set of web privacy tools [72]. There is therefore still a gap in research eliciting user responses via a complete list of tools. This is specifically helpful when significant disparities are demonstrated when the two lists (users and websites) are compared. In addition, while previous research has looked into sources of information in the security and privacy context in general [61], knowing how the users learn about tracking protection methods specifically may help assess routes to tracking protection via PETs. In this paper, we explore both aspects via user studies in Study 2.

3 Study 1: System Studies of Tracking Protection Methods

3.1 Aim

The usability of the cookie notices and other forms of tracking protection PETs (e.g. deletion of data) have been studied via user studies in [31, 77]. However, to the best of our knowledge, nobody has studied what are all forms of PETs offered by websites to the users. In [50], a list of such PETs is presented, though no statistics are given about the popularity of each method. In addition, while it has been shown that opting-out is not as straightforward as accepting the default privacy settings [31], we don't know what are the difficulties of opting-out in case a user changes mind and wants to reject the previously accepted privacy settings. In this study, we cover all these blind spots. In addition, tracking practices of different set of websites have been studied in the last few years [16, 46, 50, 53, 63, 77]. Such reports show that the common practices change over time. Hence, here we study the cookie notices of popular websites too and contribute to the knowledge of such changes.

As explained earlier, we focus on the GDPR framework which requires the service providers to (i) provide information about tracking technologies (cookies) in such a way that the user will see it when they first visit the service; usually via the cookie consent mechanism itself, (ii) separate consent from other matters and do not bundle into terms and conditions or privacy notices (iii) do not emphasise *Agree* (yes, accept, allow, etc.) over *Reject* (no, block, decline, etc.) in the cookie notice, and do not limit the options of the notice to Agree only, (iv) enable the user to withdraw that previously given consent at any time with the same ease that they gave it, and (v) do not rely on browser settings (or other mechanisms) for the user to set preferences in relation to the setting of cookies.

In this study, we visit top EU websites and study them for their privacy consent, opt-out mechanisms and other PETs under **RQ1:** *"What are the implications of opting-out of from the privacy consent as well as when the user changes mind later?"*, and **RQ2:** *"What are all sorts of user control options and other PETs offered to the user to improve their privacy in these websites?"*.

3.2 Method

We study the top 100 EU websites to observe their privacy-related content and control options from the user's point of view.

Case-study Websites: We chose 'Europe' in Alexa's region categories to search for top websites in the EU (Appendix A). The majority of these websites are also the top websites in the UK, Germany, and France. When the website required a location and language to continue, we chose UK and English. We excluded non-English websites and redundant ones and built a data set including 100 websites. These websites varied in their purposes and services, ranging from search engines and news to gaming, social media, shopping, etc. Our experiments have been conducted between Sep 2020 to Feb 2021.

Procedure and Measurement: We open each of the websites on PC on Google Chrome on a Windows

laptop and observe the following: (i) whether or not there is a cookie notice? What is the location of the notice? What are the user options included in the notice? and (ii) what is the number of clicks for rejecting (opting-out)? What is the number of clicks for opting-out after accepting the cookie consent? (iii) what are the other PETs in the privacy-related pages of the website beyond the cookie consent?

For such observations, we open each website and try to opt-out of the cookie notice and log the number of clicks. Then, we clear the browsing history and on the second visit, we accept the cookies (which is normally zero or one click). This time, we don't delete the cookie settings in the browser, and on the next visit, we try to opt-out from the previously accepted privacy consent. This may be enabled through a dedicated privacy icon in the corner of the page, or typically through the privacy-related links at the bottom of the page. To make sure that clearing the browsing history is enough for our purpose, we also ran an experiment via Google Chrome Incognito mode, Firefox Private mode and Brave– which is a privacy-oriented browser and blocks all fingerprinting activities. We get consistent results across browsers and browsing modes which reassure that browser fingerprinting does not influence the results.

For measuring the complications of opting-out, we count the number of clicks for each target. We perform those observations ourselves as 'expert users' in order to demonstrate the existing complications in the simplest form. To reduce the errors, we have tested other routes of opting-out at least twice for each website. Further investigations have been performed in case of inconsistency. During the evaluation, some patterns became more visible after visiting the first few websites and we became experienced leading to minimising errors. Other studies have adopted more advanced measurement methods (e.g. all user action such as scrolling, reading, clicking, etc.) for assessing other aspects of user privacy and via recruiting participants e.g. [31, 77], which we plan to explore in the future.

Next, we clear the browsing history again and open each website and follow the related privacy links in order to find further privacy options, links, and tools offered to the user. This is a tedious manual process and prone to errors. To improve the accuracy of our content analysis, we first try to find the privacy-related pages via the privacy consent. If we could not do so, we click on the privacy-related pages (e.g. privacy/cookie policy, interest-based ads, EU privacy rights) at the bottom of the page. After we build a list of the identified PETs, we cross-check all the items by searching our keywords in the privacy-related pages of each website again. This process is done independently by two researchers. A more detailed template that was followed for our website analysis is provided in the Appendix.

Limitations: Since in this paper we have a multidimensional purpose (system studies as well as user studies), some of our methodological choices have been influenced by such purpose. For observing the number of clicks for rejecting cookies and opting-out after accepting privacy settings, we simplify our experiment by considering an 'expert user'. We don't consider other factors such as difficulty in finding the opt-out routes, other user actions (e.g. scroll, filling text, etc.) and the spent time (e.g. similar to [31]). Most of the privacy options are normally found through the privacy-related links at the bottom of the webpage presented with small fonts. We assume our expert user knows where to look at and only count the number of clicks. In doing so, we show that even under that simplified test condition, opting-out is much more complicated than accepting the default settings. We acknowledge that by simplifying our experiments, we potentially lose further information about the usability metrics such as font size, colours, etc. However, we highlight that even under such a testing setup, dark patterns can be observed and our approach doesn't invalidate our findings.

In the future, we plan to run experiments with real users and measure the difficulties that they experience in tracking protection. In addition, we conduct this study manually since we want to investigate these websites from the user's point of view. This approach is not salable for large-scale studies. Now that we have the protection PETs keywords, we plan to use automated algorithms to conduct studies at a larger sample set in our future research. We conduct our experiments on PC browsers and do not investigate the differences on other platforms e.g. mobile browsers and mobile apps. Previous research has shown that privacy practices indeed differ across platforms [50]. We leave this as future work too. Finally, due to the dimensions of our experiments, we limit the scope of our paper by focusing on the GDPR only. While there might be some applicability to other legal frameworks, this remains as future work to investigate the same issues according to other data protection regulations such as the CCPA.

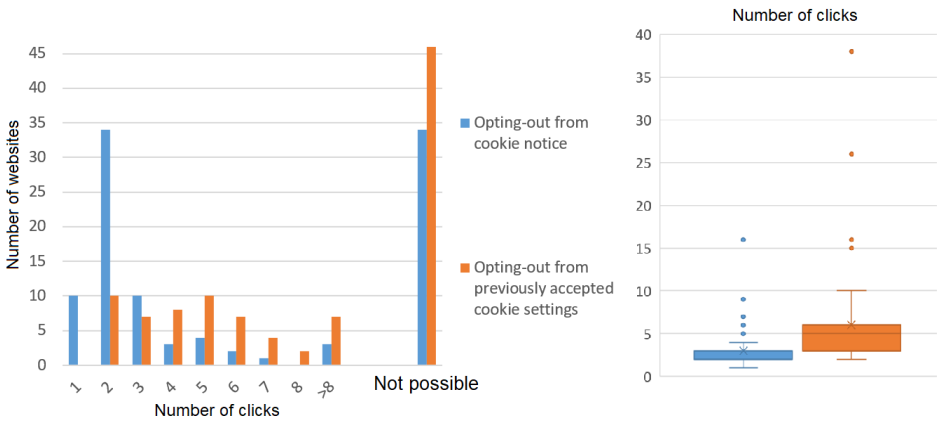

Fig. 2. Opting-out when website visited for the fist time vs. Opting-out of previously accepted settings, Left: Number of websites for each click count, Right: the distribution of number of clicks. Websites with no opt-out options are excluded from the right plot.

Control options	Other options	no. of websites
None		5
Notification		15
Only Accept		22
Highlighted Accept	Reject	3
	Options	41
Accept	Reject	3
	Options	11

Table 1. Cookie notice control options in top 100 EU websites

3.3 Results

3.3.1 Cookie Notice

As it can be seen in Table 1, 5 websites did not have any cookie notice, 15 only notified the user without any control options. 22 websites presented their cookie notice with one option only: *Accept* (agree, ok, yes, I understand, etc.). 44 websites included other options (more information, settings, customise my choices, etc.), but highlighted *Accept* over other options. Only 14 websites presented a cookie notice which included another option in addition to *Accept* where *Accept* was not highlighted. However, only three of them allowed to reject as easy as accept. Apart from the latter category, all the other practices are non-compliant with the law and do not meet the minimum requirements provided by the GDPR [37]. This rate is in the same range as what was found in the previous work [50, 53].

These cookie notices were displayed in different formats (in-page vs overlay), sizes, colours and fonts. The location varied across these websites, 15 websites showed the notice on top of the page, 48 websites presented in the lower part of the page, and 31 websites had their cookie notice in the middle of the page. 1 website presented the notification on the right side of the page. Previous research [77] shows that users are more likely to engage with a notice positioned in the lower left side of the screen in PC. This practice was observed in 3 of our websites only. However, around one third of our websites showed their cookie notices in the middle of the page (and mainly as an overlay that required user engagement before using the website). This practice has not been tested in [77] and potentially would engage the users highly. This remains as future work to be explored.

3.3.2 Opting-Out

Fig. 2 demonstrates the number of clicks for opting-out and websites (left) and the distribution (right) of the number of clicks. These plots demonstrate two test conditions: (a) opting-out of privacy consent when the website is visited for the first time and (b) when the user changes mind and wants to opt-out of previously accepted privacy settings. Out of the 100 websites, 5 did not have any cookie notice at all, 34 did not allow to opt-out through the cookie notice (shown by not possible in the left plot), and 46 would not provide an opt-out option in case of changing mind. For the remaining websites, it would take the user to opt-out from the cookie notice by 3 clicks on average. If the user accepts the cookie notice, and changes mind later, it would take them 6 clicks on average to opt-out. We observed that even when the number of clicks was low (e.g. 2 or 3) for opting-out, there are other complications for the users to opt-out. For example, they have to scroll down to find the reject option and or go to a new page for the desired privacy settings. These action items would take

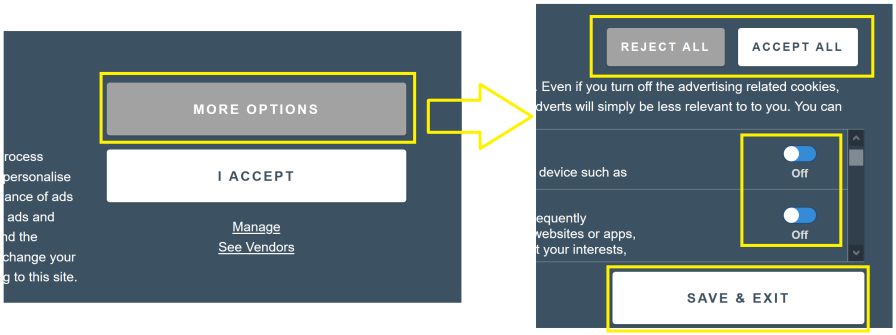

Fig. 3. Example of opting-out via cookie notice and existing violations (Accept is highlighted and cookies are pre-selected).

much more time vs opting-in. These results show that opting-out (under any circumstances) is not as easy as opting-in which normally requires the user zero or at most one click. This is another non-compliant practice that was seen on most of our websites.

When trying to opt-out of previously accepted privacy settings, the majority of the websites required the user to click on the privacy links at the bottom of the page. In some cases, the cookie notice would pop-up after clicking the privacy link, and in other cases, it would take the user to further pages. Only in three cases, there was a privacy icon presented as an overlay design (still in small size) at the bottom of the page which was visible to the user all the time while on the website. In addition, we found the same dark patterns of the cookie notices (e.g. highlighting *Accept* over *Reject*) in other areas of many websites. For example, when the user tries to opt-out via the cookie notice, in the next stages, multiple options (accept, reject, more info, etc.) are presented with similar nudging patterns (Fig. 3).

3.3.3 Available PETs

From the user's point of view, it is important to examine what further privacy-enhancing options are provided by online services. By following the related privacy links and options available in the privacy-related pages of each website (including the links in the cookie notice), we recognised that most websites provide two different pages: cookie policy and privacy policy, among other related pages. Table 2 shows these PETs and their popularity among the websites.

Contacting service provider: Almost all websites provided information for contacting them via some form of electronic communication e.g. email addresses, and online forms or links dedicated to privacy matters. Some offered other ways of communications for privacy purposes e.g. via sending an SMS including "STOP" to opt-out from receiving the advertisement.

Category	no. of websites
Contacting service provider	94
Browser settings	90
Initiatives	73
Opting-out of 3rd party websites	66
Information Commissioner's Office (ICO)	53
Website & account settings	34
Browser add-on	25
Mobile & app settings	21

Table 2. PETs offered by top 100 EU websites

Browser settings: The majority of these websites recommended that the user can prevent tracking by changing the browser settings including activating Do Not Track (DNT), deleting cookies manually, and providing links to information about how to modify settings in certain browsers such as IE, Firefox, Chrome, Safari, on PC and mobile devices. Note that according to the GDPR, relying on the user to modify the browser settings for tracking protection is not law-compliant.

Initiatives: A large number of the websites referred the user to the related initiatives including European Interactive Digital Advertising Alliance (EDAA) websites (e.g. edaa.eu or youronlinechoices.com), Interactive Digital Advertising Alliance (DAA, aboutads.info, youradchoices.com, and its mobile version: youradchoices.com/appchoices), Canadian (youradchoices.ca) and Japanese (ddai.info), Interactive Advertising Bureau (IAB) and its European version, Network Advertising Initiative (NAI, networkadvertising.org), aboutcookies.org, allaboutcookies.org, privacyshield.gov, cookielaw.org, europa.eu, cookiecentral.com, etc. This requires the user to go out of the website and visit other sources to improve their privacy.

Opting-out of 3rd-party websites: More than half of the websites provided information and links about their partners and guided the user to opt-out of them via their own website or the third party website. This included information and/or links to big companies such as Google (and Youtube), Facebook (and Instagram), and Twitter for the user to adjust their online privacy settings through these websites. This normally includes a long list of third parties and unless there is an option such as "Reject all", is not a practical method.

Information Commissioner's Office: Around half of the websites provided information, links, and email address of ICO (ico.org.uk), explaining how the user can find more information about online privacy on the ICO website and/or report certain violations and complaints to the ICO. Similar to the above categories, this also requires the user to exit the website and visit another website to improve their privacy.

Website & account settings: Around one third of the websites advised the user to change privacy preferences via the website privacy dashboard settings and user account. Some provided links, and some only mentioned this as an option. A few websites advised the user to stop using their services by deleting or deactivating the user account in order to protect their privacy.

Browser add-on: A quarter of the websites provided information (and in some cases links) to privacy-enhancing extensions to improve privacy. This was mainly a link to Google Analytics Opt-out Add-on. Ghostery was mentioned on one website.

Mobile & app settings: Some websites provided information and links about how modifying mobile devices and apps settings to change privacy preferences can improve privacy. Some of these websites provided extensive instructions such as: "When using a mobile device, you can opt-out of receiving interest-based advertising by selecting 'Privacy' and then 'Advertising' in the Settings of your Apple iPhone or iPad, or the "Opt-out of Ads Personalisation" in the Google Settings on your Android device. You may also be able to reset the unique identifier that Google uses for online behaviour-based advertising (referred to as an "Advertising ID") in the Settings on your Apple or Android device.)". Some other websites only mentioned that this is an option without further explanations and links.

As it can be seen, a wide range of options are offered to the users; supposedly to improve their privacy. Finding these options requires the user to go way beyond the first page of the website and even out of the website (and to other websites). We observed that the user has to read through multiple text-heavy privacy-related pages to be able to find the above and practice them. Some of these links are broken and the readability of content for a non-expert user is debatable. The usability of a subset of the above items has been studied in prior work [31, 32]. We plan to conduct another study to measure the accessibility and usability of the full list in our future work.

Furthermore, this study explores the top 100 EU websites. It is likely that these popular websites are well-equipped and potentially have better resources to focus on law-complaint practices. Potentially less popular websites with less human and financial resources would employ less adequate practices leading to worse tracking activities and fewer user control options. However, bigger companies have the financial resources to pay for penalty fees of potential breaches as we have seen in the last few years [35]. We leave this as future work to be explored.

4 Study 2: User Inquiry of Tracking Protection Methods

4.1 Aim

With regards to the use of PETs for tracking protection, previous research has looked into the usability of notice and choice and browser extensions [31, 43, 77] or into mental models of tracking [45], with limited mention of other factors [68]. Yet in general, beyond tracking protection (and a single tracking protection study [68]), other factors have also been shown to determine the use and deployment of PETs, including awareness of PETs and knowing that they can help [11, 62]. Therefore, to gain a better understanding of the use of particular PETs for tracking protection, in Study 2 we investigate (1) how individuals learn about PETs for tracking protection, and (2) what PETs they use, in an online survey. In particular, unawareness of privacy technologies has been highlighted as a deterrent to the adoption of PETs in previous research [11, 62, 68]. We, therefore, investigate awareness of PETs under **RQ1** "*Are individuals aware of PETs for third-party tracking (TPT) protection? How do individuals learn about PETs for tracking protection, given their gender and country differences?*" In addition, we investigate use behaviour in **RQ2** via "*What PETs do individuals use for TPT protection?*". Note that we focused on third-party tracking as the more intrusive tracking method, compared to first-party tracking.

Country	N	Mean Age	Gender		
			#F	#M	#N
United Kingdom	209	35.78	109	100	0
Germany	202	29.21	100	100	2
France	203	27.29	98	99	6

Note: for gender, F refers to female, M to male, and N to non-binary

Table 3. Participant Characteristics

4.2 Method

We conducted an online survey with $N = 614$ participants. In this section, we detail the survey methodology.

Participants: We sampled $N = 614$ participants, $N = 209$ from the UK, $N = 202$ from Germany (GE) and $N = 203$ France (FR). We chose these three countries as they have the highest number of internet users in Europe [70], and therefore a high number of users potentially exposed to online tracking. We recruited participants via Prolific Academic, a crowd-sourcing platform whose data quality has good reproducibility [55]. While the study lasted within 20 minutes, participants were renumerated at a rate of £7.5 per hour, as advised by the Prolific platform.

The study was balanced by the number of participants in each country and gender, as we noted from previous research that UK individuals may exhibit different privacy behaviour, with respect to use of PETs, compared to other countries [11], and women may also engage in different protection practices compared to men [54]. Table 3 provides a summary of the demographic details.

Procedure: The survey study was designed as follows. We provided (1) a consent form (as described in the *Ethics* section below), (2) a demographics questionnaire, (3) we elicited participants' understanding of third-party tracking, (4) provided a note on privacy technologies and elicited how participants usually learn about PETs, and (5) queried of PETs usage. Although the survey was designed in English, it was proofread by the authors, and three of their acquaintances who are not experts in the topic. In addition, the survey was piloted on Prolific platform across the three countries, where we invited the pilot participants to comment on the survey, thereby facilitating iterative enhancements.

Survey questionnaires: Participants were provided with a series of questions as detailed in the previous section. In this section, we detail the questions on elicitation of means of learning about PETs and the use of PETs, as the main focus of this study. We also provide this verbatim in the Appendix.

Awareness of PETs. To bring participants' own understanding of tracking to the fore, we first asked participants to write about their understanding of third-party tracking (TPT) as a way of inducing their mental picture. We then noted that privacy technologies, tools or features may be a means of protecting against tracking and asked participants to select how they learnt about such privacy technology, tools or features that can help to protect from third-party tracking online. We provided a 5-option closed-ended question, with the options (1) 'friend/social contact recommendation' (2) 'work/school recommendation' (3) 'privacy/cookie policy of a website' (4) 'technology blog recommendation' (5) 'news', as well as, an 'other' box to write in other sources or that they 'don't know' of PETs for tracking protection. We chose these options with inputs from previous research findings, in particular, the channel of communication via which individuals would like to learn about PETs [68] as well as their perception of social influence and support from others as encouraging the use of PETs [11, 26].

Use of PETs. To assess the usage of PETs, we provided participants with an extensive list of PETs, gathered from three sources: (1) PETs named by a similar group of participants in recent research (such as the 26 PETs identified in [11]); (2) PETs named in cookie policies, such as Google opt-out add-on and initiatives (youronlinechoices.com) or device settings [50]; and (3) PETs suggested by privacy experts. These PETs include, for instance, privacy-oriented browsers (such as Brave, Dooble browser), or extensions (such as AdGuard, Trace, Crumble). Together. these made up a list of 57 PET options. We note that the items in (1), that is the 26 general PETs, may not all protect from tracking. However, we wanted to cater for participants who may use certain technologies, with the assumption that they provide useful protection from tracking. These PETs were also named by participants recruited from a similar sample pool [11].

Ethics: This research includes collecting data from users and had full approval from [anonymous] University's Ethics Committee before the research commenced. In addition, we designed our user studies according to Menlo Report to conduct responsible research in computer science [2]. Participation in this study was completely voluntary and anonymous and our participants could drop out of it at any stage since it was conducted online. The first page of the survey gave information about the study, letting participants know that the

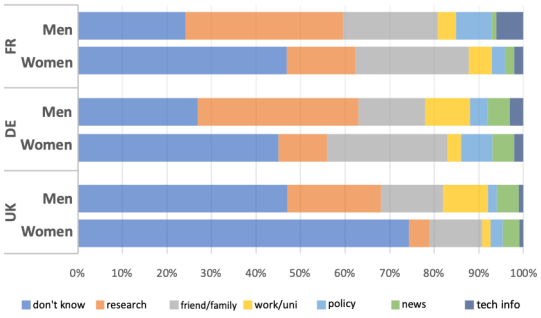

Fig. 4. % of participants learning about PETs for tracking protection via different methods.

study was anonymous, that participation was voluntary and explicitly asked for opt-in consent for participation.

Limitations: This study relied on self-reports, which is however widely employed for eliciting user responses in privacy and security user studies. We did not choose a representative sample from Prolific's sample pool, since at the time of running the study, that feature was only available for UK participants.

However, we note the difference in mean age across country groups as a limitation. We also note that there was no significant difference in age between men and women in all three countries. Future studies may endeavour towards a representative sample or to recruit from a different sample population. The study was limited to understanding usage and the path to awareness of PETs. However, the elicitation of PETs usage employed a similar question as previously used, and the list of PETs contained elements named by a similar group of participants themselves [11].

While laypersons may not be aware of all the items in the list, we expected them to identify those they use and the study was piloted with non-experts, as described in the *Procedure* section above. Overall, more research can be done into how paths to awareness and how awareness translate to the usage of PETs.

While the survey was piloted in the respective countries to invite participants feedback (on structure and comprehension), we note as a limitation that a good command of English could be correlated with higher experience in IT and security that we did not measure/elicit. The survey was written in English, and run across the UK, Germany and France.

4.3 Results

4.3.1 Awareness of PETs

We investigate RQ1 "Are individuals aware of PETs and how do they learn about PETs for tracking protection, given their gender and country differences?" We collated how participants learnt about PETs for tracking protection. While we provided participants with a close-ended question, we found additional recurring themes in participants' responses in the 'other' option. For example, some participants responded to the 'other' option with P33 *"My brother who is an IT expert"* or P396 *"my father taught me about them"*. We, therefore, extended the 'friend/social contact' category pertaining to relations and social contacts to include 'family'.

Other responses also included responses pointing to participants' own research to seek for PETs via internet searches, or finding information in webpages, such as P44 *"Found it myself through researching"* or P123 *"Reddit, Internet"*. We collated these together with the 'tech blog recommendation' category and renamed the category to own 'research'. In addition, a few participants responded to finding PETs via browser options or technology information, as P336 *"I think I discovered privacy options in browsers by myself when I was 15"* or P92 *"reading the brave browser info when installed brave [sic]"*. We coded these into the new theme 'tech info'. While the 'don't know' theme (corresponding with 44.6% participants) refers to participants who are not aware of PETs for tracking protection (as set in the questionnaire), we can additionally assume that it also contains those who do not remember how they became aware of such PETs, as a couple of participants said that they do not remember.

We provide a summary of ways individuals learn about PETs in Fig. 4. We note noticeable patterns, such as (1) a larger percentage of women said that they did not know compared to men, in all three countries; (2) finding PETs via one's own research was the most named approach of becoming aware of PETs among men in all countries, followed with learning via the support of friends and family which is also the preferred method for women; and (3) privacy policies only make up a small % of participant responses. We only report on men and women without non-binary gender. This is because the study has an almost equal number of men and women participants, thereby aiding comparison, but only has 8 participants reporting non-binary gender.

To look into the statistical effects of gender and country differences, we computed three binary logis-

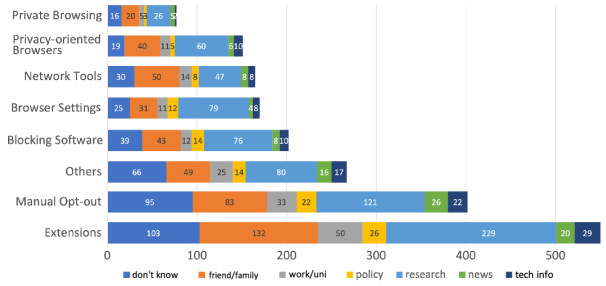

Fig. 5. Number of participants using different categories of PETs & how they learn about them.

tic regressions, one for each of the two most popular ways participants learnt about PETs ('own research' and 'friend/family') and one for 'don't know', with target variable being one of the ways and country and gender as predictors. We chose regression models over X^2 tests, as we would need a larger number of (X^2) tests with multiple comparison corrections, given our data structure.

The model with 'own research' as target variable is significant with $\chi^2(3) = 45.977$, $p < .001$, R^2 is between 10% (Cox & Snell) and 15% (Nagelkerke), where women are about 74% less likely to do their own research, and both German and French about twice more likely than UK participants. The model has an accuracy of 78%. The model with 'friend/family' as target variable is not significant, while the model with 'don't know' as target variable and country and gender as predictors, is significant with $\chi^2(3) = 70.135$, $p < .001$, R^2 is between 11% (Cox & Snell) and 15% (Nagelkerke), where women are about 2.7 times more likely to not be aware of PETs/not remember, and both German and French about 66% less likely than UK participants. The model has an accuracy of 64%.

4.3.2 Use of PETs

We investigate RQ2 "What PETs do individuals use for TPT protection?" We compute the frequency of mentions of each of the 57 PETs. We report on the PETs used by at least 10 participants, that is the 45 most used PETs, in Fig. 6. Browser extensions, such as Adblock, AdblockPlus and UBlock, are among the most popular PETs used for tracking protection. The popularity of browser extensions is consistent with the previous research; extensions are popular and often also used for UX rather than privacy [45]. However, browser extensions, as tracking protection recommendation, was only seen in 25 out of 100 websites (and mainly for Google Analytics Opt-out Add-on) in Study 1. The methods reported by our participants for tracking protection are clearly distant from those websites offer in Study 1 and there is a disparity between legal requirements and real-world practices. We group the PETs into 8 categories as shown in Table 4 and demonstrate the popularity of each category in Fig. 5. The categories refer to the type of protection for tracking and the design of the PET, such as whether they are browser extensions, privacy-oriented browsers, network tools, inbuilt browser settings, blocking software, private browsing, and manual opt-out. 'Others' correspond to PETs that do not belong to the previous categories. We find that extensions and manual opt-out, are the two most used PETs categories for tracking protection, with 'others' category taking third place – where 'others' includes technologies that are clearly not effective for tracking such as Paypal.

We note that the study participants may not be aware of the (in-)effectiveness (or the varied effectiveness across PETs), of the tracking protection methods that they use. In particular, some browser extensions may not effectively block ads and trackers [58] and may need manual configuration for effective protection [80]. In reality, malicious extension behaviour in browser extensions is a serious threat. Despite going under substantial vetting processes, some browser extensions downloaded from the official repositories (such as Chrome Web Store in Google Chrome and Add–ons in Firefox) are prone to malicious behaviour [41]. Moreover, some of the tracker–blocking extensions may implement backdoors for their own tracking activities (i.e. signing a contract with specific advertisement companies to allow tracking from their URL while blocking their competitors [29]).

The manual deletion of cookies from the browser after each time of browsing is not a feasible solution for users. However, users have the option to browse using *private browsing* (called Private mode in Firefox, Incognito in Chrome, InPrivate Browsing in Edge). In this setting, the cookies and history of the browsers will be automatically deleted when the browser is closed. This is useful when users want to stay stealthy in the context of their local device (i.e. smartphone, laptop or PC). However, private browsing would leak information about the user if a motivated attacker investigates the side–channel information such as deletion traces and dump database data [65].

For blocking software, in particular, using a VPN, the user identity (i.e. the specifics of the browser and network–related information such as IP address) is hid-

Type	Technology
Extensions	AdBlock, Adblock PLus, UBlock, NoScript, Ghostery, AdGuard DoNotTrackMe, Privacy Badger, Google Analytics Opt-out add-on, DuckDuckGo plugin, Firefox Facebook container, Firefox Lockwise, HTTPS Everywhere extension
Privacy-oriented Browsers	Brave, DuckDuckGo browser, Tor Browser and Microsoft Edge
Network Tools	Proxy, Virtual Machine, HTTPS, VPN
Browser Settings	Chrome Canary (builtin): Set Block third-party tracking, IE (builtin): Set Send DNT Request, IE (builtin): Set Block Third-Party Cookies, Safari (builtin): Set Prevent cross-site tracking, Firefox (builtin): Set Strict content blocking, Chrome (builtin): Set Send Do Not Track Request
Standalone Blocking Software	Anti-Malware, Kaspersky, Anti-Spyware, Firewall
Private Browsing	Private browsing or incognito mode option in modern browsers
Manual Opt-out	Clear cookies or opt-out of cookies, Clear browsing history, opt-out website: optout.aboutads.info, opt-out website: YourAdChoices - Youronlinechoices.com, Switch off location tracking, Opt-out of receiving emails or newsletters
Others	Paypal instead of internet banking, device/mobile/app settings, Pseudonyms, Password manager, Private social network, Encryption tools, Flash player privacy settings

Table 4. The categorization of PETs technologies employed by our participants.

den from the website server through a private server that the user is already connected to. From the server's point of view, they are responding to the requests sent from the private server, not the user [6]. The core problem with this configuration is the trust issues between the user and the private server. The private server is still able to track the user and browsing behaviour. This tracking data can be stored in the private server and sold to third–parties and/or controlled by malicious entities [23]. Thus, there must be a minimum level of trust between the user and the private server.

Built–in browser options refer to technologies that prevent tracking of the user without the need to install any third–party extensions or software packages (e.g. Anti–spyware and Anti–virus products). The track blocking starts at the time of webpage request sent by the browser. For instance, a request for loading a tracking JavaScript script is not sent from the browser at all. This will give the users the benefit of loading the webpage faster, saving bandwidth and blocking the trackers at the same time [7]. The technologies for this category fall into two groups: first, the privacy–oriented browsers (e.g. Brave Browser (brave.com), Tor Browser (torproject.org) or Duckduckgo Browser (duckduckgo.com/app) that have implemented privacy–preserving technologies in their browsing engines [69]. Second, the mainstream browsers are embedding a track blocker module in their products. For instance, Apple Safari has recently announced to include a smart track–blocking in Safari [71], and Mozilla Firefox have developed a track blocking module in recent releases [8]. The drawbacks of these technologies have not been researched extensively yet. In addition, relying on browser settings as the main method of tracking protection is not law-compliant.

We believe the *real–world competence* of these technologies in online tracking has not been thoroughly investigated yet. The effectiveness of other methods and especially those provided in websites through various initiatives have not been studied in depth too. We plan to conduct dedicated system and user studies to investigate these in our future work.

5 Discussion

In this section, based on our results, we provide recommendations for various stakeholders including service providers, PETs designers, end-users, and regulators.

5.1 Recommendations

Our findings across gender and country can support the designers and privacy educators to consider the diversity of behaviours in terms of finding PETs – hence to not only provide information out there but to guide different user groups according to their preferences, and support accessibility of PETs within users' preferred route. Researchers may also engage users in participatory studies to reveal what interventions (and their characteristics) may be more suitable for facilitating access.

Service providers: In Study 1 we found a few dark patterns and violations in the presentation of the cookie notices and user opt-out routes, some of which have been shown by others too. More specifically, previous research

has shown that the cookie notice is not effective since user choice is not even taken into consideration. In some cases, cookies are placed before the presentation of the cookie notice [46, 50, 64]. These non-compliant practices may be on purpose and/or due to careless implementation patterns such as copying and pasting program codes which contain trackers. Another example is when a website detects some form of track-blocking on the user device and refuses to provide services to the user unless the blocker is turned off. In view of all of that, we recommend that websites carefully go through their privacy practices and aim for lawful, fair, and ethical processes.

PETs designers: Study 2 reported a list of methods that may vary in their effectiveness of tracking protection, unbeknownst to users. In addition, while users' own research may be the most reported way of becoming aware of protection methods overall, this may not apply to all countries and gender, as observed in Study 2. In fact, becoming aware via social connections is a close second preferred method.

We recommend that PETs designers make it clear what protection is offered by particular PETs, in a language that matches users' limited understanding of tracking and cookies and help to clear out inaccurate mental models [45, 48, 83], as well as spell out what protections *are not* provided by particular PETs. This will help deal with misconceptions that cookies behave like viruses, and expecting anti-virus software to protect them from tracking. Designers also ought to be aware of gender and country differences in how individuals learn about PETs, and be able to cater for different groups. While more research into the accessible means of communicating PETs information to users is needed (so as not to rely solely on users to conduct their research, where the burden is on users), designers can already consider the use of social networks, since apart from this paper, other researchers have also pointed to the impact of social influence on the use of PETs [11, 26]. It would also be helpful to establish PETs repositories, and make vetted recommendations more accessible to the lay user. Existing lists include that of the Electronic Frontier Foundation's (eff.org/pages/tools) or the European Agency for Cyber Security's (enisa.europa.eu/publications/privacy-tools-for-the-general-public) (ENISA) list of privacy tools for the general public.

Users: End–users have a variety of options to restrict and/or block online tracking activities. Overall, we recommend that the users consider the privacy–oriented browsers over other options. These products are usually developed efficiently based on the established web–engines. For instance, Brave Browser has been developed based on Chromium, the open–source version of Google Chrome. Therefore, it has the efficiency capabilities of webpage rendering and JavaScript execution (e.g. V8 JavaScript Engine and Blink browser engine) and the ability to install WebExtensions-based browser extensions. Meanwhile, the user will be protected against tracking with a built–in track blocker with minimum impact on the page loading time. Other ways to improve user privacy experience is via education (e.g. free online courses, and reliable sources such as the ICO [37]), managing privacy settings across their user accounts, and practising their data privacy right via contacting service providers and other related entities.

Users may also be encouraged to openly share about their experiences of privacy protection online, via social networks or other ways, so as to scale the potential impact of social influence and trusting connections on the use of PETs. This would also facilitate the development of more privacy-empowered online communities.

5.2 Online Privacy Regulations

Our findings highlight that people across gender and country indeed perceive and protect their privacy differently, and hence regulators should identify those needs leading to more effective and sometimes distinctive regulations. Another dimension is the purpose of tracking. Evidently, the tracking industry managed to impact political decisions by deploying effective micro-targeting advertisements. The regulators should consider updating laws to address the specific misuses of collected tracking data. For instance, the laws should be clear on the micro-tracking advertisement with political contents [22]. We discuss that instead of general regulations, multiple dimensions should be taken into account for more effective legislation. Such dimensions include tracking across demographics, nationalities, and purposes. ICO has already started setting specific guidelines for different key data protection themes concerning children, age, and AI [36]. Such efforts should be extended to more contexts.

The research community has now well researched the dark patterns that exist in common practices by vendors. Our results demonstrate that the PETs offered by the websites, those that users employ and the ways that they learn about them do not match. In addition, very few websites follow law-compliant approaches. One might wonder how better enforcement of data protec-

tion regulations is possible when such a wide range of violations exists in the real-world. As mentioned before, many companies have been and are violating the data protection regulations and pay the penalty fees [35]. There are several national data protection authorities across the world who support the enforcement of privacy laws. For instance, ICO in the UK covers a few legislation including the GDPR [38]. Among the other services that such data protection authorities can offer (e.g. report a breach, make a complaint, and pay fees), they provide a set of technical guidelines translating legal requirements to technical terms (e.g. cookie notice requirements [37]).

We envision that user privacy will become significantly concerning on other platforms such as mobile websites and apps and IoT devices as recognised by previous research [50, 78]. Some efforts have been recently made for app privacy by companies such as Apple and Google. Here, we explain Apple's App Tracking Transparency (ATT) policy [17] as an example of industry self-regulation. Apple's recent ATT policy, on iOS 14.5 (26 April 2021), requires developers to ask for permission when they use certain information from other companies' apps and websites for advertising purposes, even if they already have user consent. This is a significant effort into making app tracking activities more limited, though, it comes with its own complications. For example, it means iPhone owners are now seeing much more privacy prompts as they continue using their regular apps, each one asking for permission to "track your activity across other companies' apps and websites", with two options on the notices as "Ask App not to Track", and "Allow", in addition to the app name to be shown in the Tracking menu within user broader iOS Privacy settings, for further manual settings. Furthermore, it may be challenging for Apple to actually enforce parts of its ATT policy such as restricting the app to use other user identifiers (such as hashed email addresses). Interestingly, some recent reports show that 96% of US users opt-out of app tracking introduced in iOS 14.5 [73]. Since the enforcement of this policy is relatively recent, various aspects of its effectiveness in improving user privacy remains unresearched. Google is also working on a similar privacy feature for its Google Play Store and apps, however, the details of this plan are not clear yet [81].

In view of all of the above, we believe that the research community should continue to research this field and especially the blind spots such as data concerning 'marginalised user groups' on all platforms i.e. PC, mobile and IoT. Through strong collaboration between the regulators and researchers, a proactive approach can be taken into account in order to protect user privacy more efficiently; allowing all user groups to use online technologies without risk and fear.

6 Conclusion

Online tracking is messy and complex from all perspectives i.e. tracking methods, protection technologies, regulations, and user dimensions. Privacy-enhancing tools and methods can help Internet users protect themselves on online platforms. However, the complexity in the regulations, their implementation, and enforcement, as well the wide range of tools available for the users to be employed make it difficult for them to adopt such tools effectively. To shed light on the disparities between the legal requirements for tracking protection, websites and user practices, we conducted multi-dimensional research. We designed experiments to investigate protection from online tracking via conducting two studies looking into websites and users, respectively. In Study 1, we first looked at cookie notice presentation and control options in 100 top EU websites, then we evaluated the difficulties to opt-out in two situations: 1) when the user visits the websites for the first time, and 2) when the user changes mind and what to opt-out of previously accepted privacy settings. In Study 2, we surveyed 614 users in the UK, Germany, and France and asked them if and how they protect from online tracking. We also asked them how do they learn about these protection methods (e.g. via research, friends and family, etc.).

We showed that opting-out is not as straightforward as accepting the default privacy settings, and becomes even more complicated when users want to opt-out from previously accepted privacy settings. We also found that the protection methods users employ do not necessarily tie up with the PETs offered by online service providers and some of the methods practised by the users do not prevent tracking at all. This paper touches on both system and user aspects and synthesizes findings to present an alarming disparity between privacy regulations, website practices of presenting PETs in the real-world, and how users learn about PETs and practice them. Such a disparity sheds light on why current policies and practices are ineffective in supporting the use of PETs by users. Our studies show that there is an urgent need to address the gaps in this space, not only by researchers, but also by the policymakers, service providers, and PETs designers.

7 Acknowledgements

We would like to thank the participants of our user studies. We thank the PoPETs reviewers for their constructive feedback on this paper. This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

[1] W. Alcorn, C. Frichot, and M. Orru. *The Browser Hacker's Handbook*. John Wiley & Sons, 2014.

[2] M. Bailey, D. Dittrich, E. Kenneally, and D. Maughan. The menlo report. *IEEE Security & Privacy*, 10(2):71–75, 2012.

[3] H. Beales. The value of behavioral targeting. *Network Advertising Initiative*, 1:2010, 2010.

[4] Z. Benenson, A. Girard, and I. Krontiris. User acceptance factors for anonymous credentials: An empirical investigation. In *WEIS*, 2015.

[5] G. Blank, W. H. Dutton, and J. Lefkowitz. Perceived threats to privacy online: The internet in britain, the oxford internet survey, 2019. 2019.

[6] T. Braun, M. Günter, M. Kasumi, and I. Khalil. Virtual private network architecture. *Charging and Accounting Technology for the Internet (Aug. 1, 1999)(VPNA)*, 1999.

[7] Brave. *Accurately Predicting Ad Blocker Savings*, 2019.

[8] D. Camp. *Firefox Now Available with Enhanced Tracking Protection by Default ...*, 2019.

[9] B. Chandramouli, J. Goldstein, X. Jin, B. S. Raman, and S. Duan. Real-time-ready behavioral targeting in a large-scale advertisement system, May 14 2013. US Patent 8,442,863.

[10] E. Commission. Special eurobarometer 431: Data protection, 2015.

[11] K. P. Coopamootoo. Usage patterns of privacy-enhancing technologies. In *ACM CCS*, 2020.

[12] L. F. Cranor, H. Habib, y. Zou, A. Acquisti, J. Reidenberg, N. Sadeh, and F. Schaub. Design and evaluation of a usable icon and tagline to signal an opt-out of the sale of personal information as required by ccpa. 2020.

[13] A. Das, G. Acar, N. Borisov, and A. Pradeep. The web's sixth sense: A study of scripts accessing smartphone sensors. In *ACM CCS*, 2018.

[14] L. de la Torre. A guide to the california consumer privacy act of 2018. *Available at SSRN 3275571*, 2018.

[15] P. De Ryck, L. Desmet, F. Piessens, and M. Johns. *Primer on client-side web security*. Springer, 2014.

[16] M. Degeling, C. Utz, C. Lentzsch, H. Hosseini, F. Schaub, and T. Holz. We value your privacy... now take some cookies: Measuring the gdpr's impact on web privacy. In *NDSS*, 2018.

[17] A. Developer. *App Tracking Transparency*, 2021.

[18] B. G. Edelman and M. Luca. Digital discrimination: The case of airbnb. com. *Harvard Business School NOM Unit Working Paper*, (14-054), 2014.

[19] S. Englehardt and A. Narayanan. Online tracking: A 1-million-site measurement and analysis. In *ACM CCS*, pages 1388–1401, 2016.

[20] ENISA. Privacy enhancing technologies, 2020.

[21] J. Estrada-Jiménez, J. Parra-Arnau, A. Rodríguez-Hoyos, and J. Forné. Online advertising: Analysis of privacy threats and protection approaches. *Computer Communications*, 100, 2017.

[22] L. Fernandez. Digital advertising in political campaigns and elections. In *A Research Agenda for Digital Politics*. Edward Elgar Publishing, 2020.

[23] H. Field. *Hundreds of Millions Have Downloaded Suspicious VPN Apps With Serious Privacy Flaws. Apple and Google Haven't Taken Action*, 2019 (Sep 16, 2020).

[24] Forbes-Insights. Rethinking privacy in the ai era, 2019.

[25] K. Garimella, O. Kostakis, and M. Mathioudakis. Ad-blocking: A study on performance, privacy and counter-measures. In *ACM Web Science Conference*, pages 259–262, 2017.

[26] N. Gerber, V. Zimmermann, and M. Volkamer. Why johnny fails to protect his privacy. In *IEEE EuroS&P*, pages 109–118. IEEE, 2019.

[27] A. Gervais, A. Filios, V. Lenders, and S. Capkun. Quantifying web adblocker privacy. In *European Symposium on Research in Computer Security*, pages 21–42. Springer, 2017.

[28] A. Gómez-Boix, P. Laperdrix, and B. Baudry. Hiding in the crowd: an analysis of the effectiveness of browser fingerprinting at large scale. In *world wide web conference*, pages 309–318, 2018.

[29] J. Greenberg. *Ad Blockers Are Making Money Off Ads (And Tracking, Too)*, 2016 (Sep 16, 2020).

[30] G. Greenleaf. Global data privacy laws 2019: 132 national laws & many bills. 2019.

[31] H. Habib, S. Pearman, J. Wang, Y. Zou, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub. It's a scavenger hunt: Usability of websites' opt-out and data deletion choices. In *CHI*, 2020.

[32] H. Habib, Y. Zou, A. Jannu, N. Sridhar, C. Swoopes, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub. An empirical analysis of data deletion and opt-out choices on 150 websites. In *SOUPS*, 2019.

[33] D. Harborth and S. Pape. Examining technology use factors of privacy-enhancing technologies: the role of perceived anonymity and trust. 2018.

[34] M. Hatamian. Engineering privacy in smartphone apps: A technical guideline catalog for app developers. *IEEE Access*, 2020.

[35] ICO. *Enforcement action*, 2021.

[36] I. C. O. (ICO). Age appropriate design: a code of practice for online services. *ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/*, 2020.

[37] I. C. O. (ICO). How do we comply with the cookie rules? *ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/how-do-we-comply-with-the-cookie-rules/ May 2020.*, 2020.

[38] I. C. O. (ICO). Ico legislation cover. *https://ico.org.uk/about-the-ico/what-we-do/legislation-we-cover/*, 2021.

[39] M. Ikram, R. Masood, G. Tyson, M. A. Kaafar, N. Loizon, and R. Ensafi. The chain of implicit trust: An analysis of the web third-party resources loading. In *World Wide Web Conference*, 2019.

[40] A. Inc. *Safari 12.1 Release Notes*, 2019 (Sep 16, 2020).

[41] N. Jagpal, E. Dingle, J.-P. Gravel, P. Mavrommatis, N. Provos, M. A. Rajab, and K. Thomas. Trends and lessons from three years fighting malicious extensions. In *USENIX*, pages 579–593, 2015.

[42] B. Krishnamurthy and C. Wills. Privacy diffusion on the web: a longitudinal perspective. In *World wide web Conference*, pages 541–550, 2009.

[43] P. Leon, B. Ur, R. Shay, Y. Wang, R. Balebako, and L. Cranor. Why johnny can't opt out: a usability evaluation of tools to limit online behavioral advertising. In *ACM CHI*, 2012.

[44] P. G. Leon, A. Rao, F. Schaub, A. Marsh, L. F. Cranor, and N. Sadeh. Privacy and behavioral advertising: Towards meeting users' preferences. In *SOUPS*, 2015.

[45] A. Mathur, J. Vitak, A. Narayanan, and M. Chetty. Characterizing the use of browser-based blocking extensions to prevent online tracking. In *SOUPS*, pages 103–116, 2018.

[46] C. Matte, N. Bielova, and C. Santos. Do cookie banners respect my choice? measuring legal compliance of banners from iab europe's transparency and consent framework. *IEEE S&P Conference*, 2019.

[47] J. R. Mayer and J. C. Mitchell. Third-party web tracking: Policy and technology. In *2012 IEEE Symposium on Security and Privacy*, pages 413–427. IEEE, 2012.

[48] A. McDonald and L. F. Cranor. Beliefs and behaviors: Internet users' understanding of behavioral advertising. Tprc, 2010.

[49] S. Medvedev et al. Data protection in russian federation: overview. *Thomson Reuters Practical Law*, 2016.

[50] M. Mehrnezhad. A cross-platform evaluation of privacy notices and tracking practices. In *EuroUSEC*, 2020.

[51] G. Merzdovnik, M. Huber, D. Buhov, N. Nikiforakis, S. Neuner, M. Schmiedecker, and E. Weippl. Block me if you can: A large-scale study of tracker-blocking tools. In *IEEE EuroS&P*, 2017.

[52] N. Momen, M. Hatamian, and L. Fritsch. Did app privacy improve after the gdpr? *IEEE Security & Privacy*, 17(6), 2019.

[53] M. Nouwens, I. Liccardi, M. Veale, D. Karger, and L. Kagal. Dark patterns after the gdpr: Scraping consent pop-ups and demonstrating their influence. In *CHI*, pages 1–13, 2020.

[54] Y. J. Park. Do men and women differ in privacy? gendered privacy and (in) equality in the internet. *Computers in Human Behavior*, 50:252–258, 2015.

[55] E. Peer, L. Brandimarte, S. Samat, and A. Acquisti. Beyond the turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, 70:153–163, 2017.

[56] E. Pernot-Leplay. China's approach on data privacy law: A third way between the us and the eu? *Journal of Law & International Affairs*, 8(1), 2020.

[57] G. Pugliese, C. Riess, F. Gassmann, and Z. Benenson. Long-term observation on browser fingerprinting: Users' trackability and perspective. *Privacy Enhancing Technologies*, 2020(2):558–577, 2020.

[58] E. Pujol, O. Hohlfeld, and A. Feldmann. Annoyed users: Ads and ad-block usage in the wild. In *Internet Measurement Conference*, pages 93–106, 2015.

[59] A. Razaghpanah, R. Nithyanand, N. Vallina-Rodriguez, S. Sundaresan, M. Allman, C. Kreibich, and P. Gill. Apps, trackers, privacy, and regulators: A global study of the mobile tracking ecosystem. *NDSS*, 2018.

[60] J. Reardon, Á. Feal, P. Wijesekera, A. E. B. On, N. Vallina-Rodriguez, and S. Egelman. 50 ways to leak your data: An exploration of apps' circumvention of the android permissions system. In *USENIX*, pages 603–620, 2019.

[61] E. M. Redmiles, S. Kross, and M. L. Mazurek. How i learned to be secure: A census-representative survey of security advice sources and behavior. In *ACM CCS*, page 666–677, New York, NY, USA, 2016.

[62] K. Renaud, M. Volkamer, and A. Renkema-Padmos. Why doesn't jane protect her privacy? In *Symposium on Privacy Enhancing Technologies Symposium*, pages 244–262. Springer, 2014.

[63] I. Sanchez-Rola, M. Dell'Amico, P. Kotzias, D. Balzarotti, L. Bilge, P.-A. Vervier, and I. Santos. Can i opt out yet? gdpr and the global illusion of cookie control. In *ACM Asia Computer and Communications Security*, 2019.

[64] C. Santos, N. Bielova, and C. Matte. Are cookie banners indeed compliant with the law? deciphering eu legal requirements on consent and technical means to verify compliance of cookie banners. *arXiv preprint arXiv:1912.07144*, 2019.

[65] K. Satvat, M. Forshaw, F. Hao, and E. Toreini. On the privacy of private browsing–a forensic approach. In *Data Privacy Management and Autonomous Spontaneous Security*, pages 380–389. Springer, 2013.

[66] F. Schaub, A. Marella, P. Kalvani, B. Ur, C. Pan, E. Forney, and L. F. Cranor. Watching them watching me: Browser extensions impact on user privacy awareness and concern. In *USEC*, pages 1–10, 2016.

[67] M. Schunter. *Tracking Preference Expression (DNT)*, 2019 (Sep 16, 2020).

[68] F. Shirazi and M. Volkamer. What deters jane from preventing identification and tracking on the web? In *Workshop on Privacy in the Electronic Society*, 2014.

[69] P. Snyder. Next steps for browser privacy: Pursuing privacy protections beyond extensions. Burlingame, CA, Jan. 2019. USENIX Association.

[70] Statista. Number of internet users in european countries as of june 2019, 2019.

[71] N. Statt. *Apple updates Safari's anti-tracking tech with full third-party cookie blocking*, 2020 (Sep 16, 2020).

[72] P. Story, D. Smullen, Y. Yao, A. Acquisti, L. F. Cranor, N. Sadeh, and F. Schaub. Awareness, adoption, and misconceptions of web privacy tools. *PoPETs*, 2021.

[73] A. Technica. *96% of US users opt out of app tracking in iOS 14.5, analytics find*, 2021.

[74] P. Tigas, S. T. King, B. Livshits, et al. Percival: Making in-browser perceptual ad blocking practical with deep learning. *arXiv preprint arXiv:1905.07444*, 2019.

[75] M. Trevisan, S. Traverso, E. Bassi, and M. Mellia. 4 years of eu cookie law: Results and lessons learned. *Proceedings on Privacy Enhancing Technologies*, 2019(2):126–145, 2019.

[76] T. Urban, M. Degeling, T. Holz, and N. Pohlmann. Beyond the front page: Measuring third party dynamics in the field.

In *Web Conference 2020*, 2020.

[77] C. Utz, M. Degeling, S. Fahl, F. Schaub, and T. Holz. (un) informed consent: Studying gdpr consent notices in the field. In *ACM CCS*, 2019.

[78] J. Varmarken, H. Le, A. Shuba, A. Markopoulou, and Z. Shafiq. The tv is smart and full of trackers: Measuring smart tv advertising and tracking. *Privacy Enhancing Technologies*, 2020.

[79] P. Voigt and A. Von dem Bussche. The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 2017.

[80] C. E. Wills and D. C. Uzunoglu. What ad blockers are (and are not) doing. In *IEEE Workshop on Hot Topics in Web Systems and Technologies*. IEEE, 2016.

[81] xda developers. *Google Play Store's new Safety section will show you how apps use your data*, 2021.

[82] Z. Yang and C. Yue. A comparative measurement study of web tracking on mobile and desktop environments. *Privacy Enhancing Technologies*, 2020.

[83] Y. Yao, D. Lo Re, and Y. Wang. Folk models of online behavioral advertising. In *ACM Conference on Computer Supported Cooperative Work and Social Computing*, pages 1957–1969, 2017.

[84] M. Zalewski. *The tangled Web: A guide to securing modern web applications*. No Starch Press, 2012.

A Top 100 EU Websites for Study 1

Table 5 lists the most used websites in the EU countries as reported by Alexa in Sep 2020.

no.	Website	no.	Website	no.	Website	no.	Website	no.	Website
1	Amazon.co.uk	21	Www.gov.uk	41	Royalmail.com	61	Rightmove.co.uk	81	Virginmedia.com
2	Theguardian.com	22	Express.co.uk	42	Aruba.it	62	Tnt.com	82	Currys.co.uk
3	Bbc.co.uk	23	Euronews.com	43	United.com	63	Theoutnet.com	83	Topshop.com
4	Who.int	24	Oup.com	44	Next.co.uk	64	Selfridges.com	84	Chrono24.com
5	Google.co.uk	25	Search.yahoo.com	45	Bt.com	65	Johnlewis.com	85	Itv.com
6	Webex.com	26	Eset.com	46	Rte.ie	66	Thetimes.co.uk	86	Quidco.com
7	Edition.cnn.com	27	Britishcouncil.org	47	Tesco.com	67	Fxstreet.com	87	Easyjet.com
8	Dailymail.co.uk	28	Sky.com	48	Newsnow.co.uk	68	Dailystar.co.uk	88	Hsbc.com
9	Rt.com	29	Sap.com	49	Voanews.com	69	Asda.com	89	Sainsburys.co.uk
10	Asos.com	30	Mirror.co.uk	50	Childrensalon.com	70	Ucas.com	90	Riverisland.com
11	Cambridge.org	31	Weforum.org	51	Thelancet.com	71	Here.com	91	Macworld.co.uk
12	Ebay.co.uk	32	Metro.co.uk	52	Babyshop.com	72	Standard.co.uk	92	Serif.com
13	Reuters.com	33	News.sky.com	53	Argos.co.uk	73	Wipo.int	93	Harveynichols.com
14	Bet365.com	34	Jdsports.co.uk	54	Skysports.com	74	Gumtree.com	94	Yougov.com
15	Dw.com	35	Ubs.com	55	Channel4.com	75	Brownsfashion.com	95	Aeroflot.ru
16	Hm.com	36	Economist.com	56	Ryanair.com	76	Prnewswire.com	96	Nme.com
17	Ft.com	37	Espncricinfo.com	57	Irishtimes.com	77	Newscientist.com	97	Active.com
18	Telegraph.co.uk	38	Thomann.de	58	Advfn.com	78	Radiotimes.com	98	Indeed.co.uk
19	Independent.co.uk	39	Cosmopolitan.com	59	Siemens.com	79	Hotukdeals.com	99	Meltwater.com
20	Thesun.co.uk	40	Nhs.uk	60	Lyst.co.uk	80	Harrods.com	100	Nokia.com

Table 5. Top 100 EU websites

B Website Analysis Template for Study 1

For each website in our list, we followed these steps for our analysis:

- **Step 1: Visit website:** Open Google Chrome on laptop, clear browsing data via browser settings, visit the homepage of the website.
- **Step 2: Cookie notice:** Observe if there is a notice (cookie consent, privacy settings, banner, etc.).
  - No: Write it in the file.
  - Yes: Observe the location and user control options e.g. OK, Accept, Yes, Reject, No, More Options, Settings, Links to privacy-related pages, etc. Write your observations in the file.
- **Step 3: Opting-out on the first visit:** Try to opt-out from the cookie notice and count the number of clicks. If not possible, write 'NA' in the file.
- **Step 4: Opting-out of previously accepted cookies**:
  - Open Google Chrome on laptop, clear browsing data via browser settings, visit the homepage of the same website.
  - Accept the cookie notice. Close the website. Open it again without clearing the browsing history.
  - Try to opt-out of previously accepted cookie settings and count the number of clicks. This can be either via a privacy icon somewhere in the website or via privacy-related links at the bottom of the page. If not possible, write 'NA' in the file.
- **Step 5: Available PETs**:
  - Open Google Chrome on laptop, clear browsing data via browser settings, visit the homepage of the same website. Click on all the privacy-related links and options and open them in new browser tabs. This can

be via control options and links in the cookie notice, as well as privacy-related links at the bottom of the page (e.g. privacy/cookie policy, interest-based ads, EU privacy rights).
  - Parse the content of each page and look for privacy-enhancing options, tools and links. Continue clicking on the related pages and open them in new tabs until all privacy pages are visited. Write all the observed PETs in the file.
  - For double-checking, search for the following keywords in these pages: 'contact', 'browser', 'third party', 'Information Commissioner Officer', 'website settings', 'account', 'add-on', 'plug-in', 'mobile', 'app', and certain third parties and initiatives as listed in Section 3.3.3.
- **Step 6: Further observations:** Write any other observations about this website in the file.

C Questionnaires for Study 2

C.1 Demographics

What is your gender? ☐ female ☐ male ☐ non-binary
What is your age?

C.2 Awareness of PETs

Privacy technologies, tools or features can protect from third-party tracking online (henceforth referred to as PETs-TPT). Examples include browser settings or add-ons and plugins.
How did you learn about PETs-TPT?

Please select one of the options below or enter how you learnt PETs-TPT in the 'other' box. If you don't know about PETs-TPT, please answer 'I don't know' in the 'other' box.
☐ friend / social contact recommendation
☐ work / school recommendation
☐ privacy/cookie policy of a website
☐ news
☐ other (please specify)

C.2.1 Use of PETs

Below is a list of technologies that can provide privacy protection online. Please indicate the one/s you currently use specifically to protect from browser-based third-party tracking.

If you use a different technology or technologies, please name them in the other box. If you don't use any, please write NONE in the other box.

[We provide the list in compact form here for space reason.] ☐ Firefox (builtin) Set *Strict Content Blocking* ☐ Safari (builtin) Set *Prevent cross-site tracking* ☐ Chrome (builtin): Set *Send Do Not Track Request* ☐ Chrome Canary (builtin): *Set Block third-party tracking* ☐ Internet Explorer (builtin): *Set Send DoNotTrack Request* ☐ Internet Explorer (builtin): *Set Block Third-Party Cookies option or Block All Cookies option* ☐ Private Browsing or browser incognito mode ☐ Firefox Facebook container ☐ Firefox Lockwise ☐ Disconnect ☐ Ghostery ☐ AdBlock ☐ Adblock Plus ☐ UBlock ☐ Privacy Badger ☐ DoNotTrackMe ☐ DuckDuckGo plugin ☐ DuckDuckGo browser ☐ Tor browser ☐ Microsoft Edge ☐ Brave ☐ EPIC browser ☐ Dooble browser ☐ ungoogled-chromium ☐ GNU IceCat ☐ StratPage ☐ Encryption tools ☐ Clear browsing history ☐ Pseudonyms ☐ Clear cookies or opt-out of cookies ☐ Switch off location tracking ☐ HTTPS ☐ Private social network ☐ Proxy ☐ IP Hider ☐ Virtual Machine ☐ NoScript ☐ Firewall ☐ VPN ☐ Password manager ☐ Paypal instead of internet banking ☐ Anti-Spyware ☐ Anti-Malware ☐ Kapersky ☐ Opt-out of receiving emails or newsletters ☐ Google Analytics Opt-out add-on ☐ opt-out website: YourAdChoices - Youronlinechoices.com ☐ opt-out website: optout.aboutads.info ☐ Microsoft

privacy dashboard ☐ Flash player privacy settings ☐ HTTPS Everywhere extension ☐ CanvasFingerprintBlock/ Canvas Defender/ Canvas Blocker ☐ Trace ☐ Crumble ☐ AdGuard ☐ uMatrix ☐ device/mobile settings/app settings

D Participants' Use of PETs in Study 2

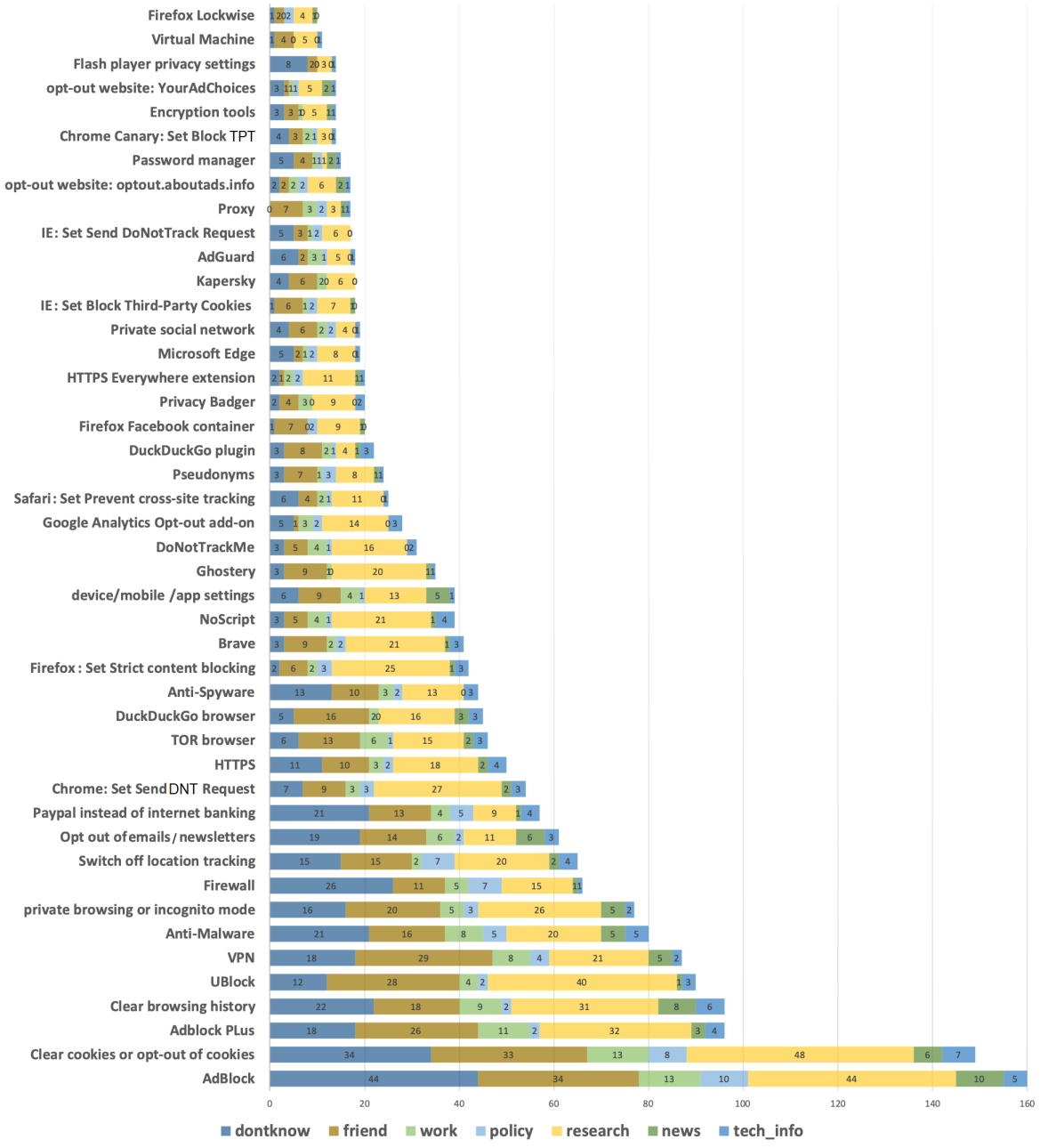

Fig. 6. Participants' use of PETs by technology type and how they learn about them (x-axis shows number of participants)